

*REMARKS/ARGUMENTS*

In response to the Office Action mailed July 14, 2005, Applicants amend their application and request reconsideration. In this Amendment claims 1-3 and 8-10 are cancelled and new claims 15-20 are added so that claims 4-7 and 11-20 are now pending.

Claim 10 was objected to because of the use of a particular phrase and all examined claims were rejected as indefinite based upon language in examined claims 1, 9, and 10. The objection and rejections as to form are all moot in view of the cancellation of the claims to which those rejections were directed. In this Amendment claims 1-3 are replaced by claim 15, claim 9 is replaced by claim 18, and claim 10 is replaced by claim 20.

The invention is directed to a system and method of ensuring a desired level of accuracy in a system that identifies whether a person supplying biometric indicia is recognized. Biometric indicia means information relating to physical characteristics of the person. Examples identified in the patent application are fingerprints, iris of the eye, face, palm, voice, and signature. These indicia are not readily reproduced by an imposter who seeks to be recognized by the authentication system in order to gain an access, for example to a room or a computer system or program. This kind of authentication system is desired over systems involving passwords or IC cards which may be copied, stolen, or imitated to gain access.

The difficulty with systems employing biometric indicia is the inherent error in collecting the indicia. For example, when a fingerprint is employed, the quality of the image captured depends upon many external conditions, including the condition of the skin, such as the presence of contaminants, moisture, oils, and injuries that lead to inaccuracies in the image. In such systems, an image captured in real time is compared to a stored image that has been captured at an earlier time, possibly under different conditions leading to variations in comparison results. A person may be correctly identified from the comparison, falsely identified, correctly rejected, or falsely rejected. The same errors inherently exist in comparing other stored and newly captured biometric indicia such as an image of an iris of the eye, a face image, a palm image, a voice sample, and a personal signature. Therefore, in some instances, a test of a single biometric index might not be sufficiently accurate to identify a person with the degree of assurance needed. Moreover, different degrees of security may require different levels of accuracy in confirming that a person supplying

biometric data is the same person who earlier supplied reference biometric data that is stored within the system for use in comparison to indicia captured currently.

The invention solves these problems by providing multiple authentication devices that capture respective biometric indicia. For example, one such device might capture a fingerprint image, another an iris image, another a second fingerprint image, and still another may capture a face image. Even if exact matches cannot be obtained between a particular captured biometric index and a corresponding reference index, by making multiple comparisons of contemporaneously captured biometric indicia, a required degree of assurance that the person supplying the biometric data is a particular person registered in the system can be attained. Stated another way, less than 50% identification accuracy may be inadequate if a single biometric index is tested to meet a moderate level of assurance of identification, for example, to permit access at a relatively low security level. However, that level of accuracy of identification of a person with respect to each of several indicia may be sufficient in the aggregate to establish the degree of accuracy needed for a particular high level of security, i.e., access.

The solution provided by the invention, as described multiple times in the patent application from page 8 to page 33, is a system with a plurality of authentication devices that collect respective biometric indicia from a person seeking access. Further, the system provides an input means, such as a keyboard, for inputting and storing accuracy thresholds for each of the authentication devices. Specifying the accuracy thresholds causes the error rates of the authentication devices to be established at particular levels as described in connection with Figures 4A and 4B of the patent application. The system also provides for input of a target identification accuracy for the system. This target identification accuracy permits the administrator of this system to establish different levels of security for different degrees of access. Higher security means that the identification accuracy must be higher so that no persons or very few persons are granted access to which they are not entitled. Further, a very important aspect of the invention is that system calculates, considering the accuracy thresholds for each of the authentication devices, the identification accuracy for the respective authentication devices as well as for combinations of those devices. Then, based upon the calculated identification accuracies of the individual authentication devices and combinations of authentication devices, the system selects for use in a particular application only those individual authentication devices or only the combinations of the individual

authentication devices that meet the minimum system target identification accuracy that has been input.

The system according to the invention is described in new claim 15. The operation of the system, both in terms of selection of the individual authentication devices, if any, and combinations of authentication devices, if any, that provide the desired level of system accuracy is described in new claim 18. Further, a method of identifying a particular person, based upon a data base of persons with registered biometric indicia, is described in new independent claim 20. The examined claims still pending have been amended to conform to these new independent claims.

As described in the patent application and in new claims 16, 19, and 21, the system administrator may impose additional limiting constraints on which of the authentication devices or combinations of authentication devices may be employed in a particular circumstance.

Claims 1-14, all of the examined claims, were rejected as anticipated by Batson et al. (U.S. Patent Publication 2002/0169874, hereinafter Batson) and as anticipated by Kawan et al. (U.S. Patent Publication 2001/0049785, hereinafter Kawan). These rejections are respectfully traversed as to the claims now presented.

Neither Batson nor Kawan describes or suggests the concept of calculating the identification accuracy of individual authentication devices and of combinations of the authentication devices, nor selecting for the system, based upon the calculated accuracies, only those authentication devices and/or combinations of authentication devices that provide an identification accuracy meeting a target identification accuracy input by an administrator of the system.

Batson describes a system that, based upon verification of various information provided by a system user, decides whether to grant access to a requested service based upon the authorization of the user and the security level of the access requested. Examples of information gathered to determine whether to grant access are the type and ownership of a computer through which access is sought, communication channel features such as encryption, passwords, and the like. None of these data that are collected in the examples of Batson are biometric indicia, although Batson makes reference to using biometric indicia without much detail. Thus, Batson does not even address the problem solved by the invention, namely dealing with biometric indicia that are subject to variation in the collection

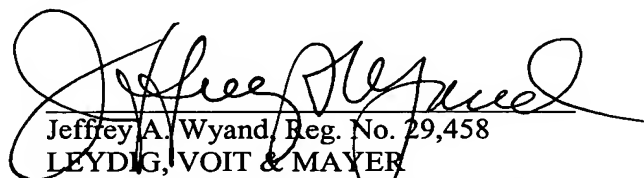
of the indicia at different times for reference and for identification purposes. While various levels of security may be assigned, based upon different security data in Batson, there is no calculation of any identification accuracy or establishment of which combinations of information data provide an accurate authentication of personal identify to determine whether access will be granted. Accordingly, Batson cannot anticipate any claim now pending.

Kawan describes a system in which a user is identified through the collection and processing of biometric indicia. In the examples of Kawan, the biometric indicia are fingerprints that are used in combination with non-biometric indicia, such as a personal identification number, passport, or digital signature, to identify a particular user. Although Kawan's system employs biometric indicia, the emphasis in Kawan is in collecting multiple fingerprints presented for particular fingers in a required sequence as a check on the accuracy of identification of a person.

Like Batson, Kawan never calculates identification accuracy of individual authentication devices or of combinations of authentication devices and never subsequently selects, based upon these calculated identification accuracies, authentication devices or combinations of authentication devices that will produce the desired level of security in identifying a person supplying the indicia. To be sure, paragraph [0032] of Kawan, cited in the Office Action, alludes to the problem of inaccuracies in capturing biometric indicia. However, Kawan's response, as described in that paragraph, is to collect mixed biometric indicia and non-biometric information *in a proper sequence* to achieve a desired identification accuracy. There is no calculation and no selection as in the invention. Accordingly, Kawan cannot anticipate nor suggest any claim now pending.

Prompt issuance of a Notice of Allowance is earnestly solicited.

Respectfully submitted,



Jeffrey A. Wyand, Reg. No. 29,458

LEYDIG, VOIT & MAYER

700 Thirteenth Street, N.W., Suite 300

Washington, DC 20005-3960

(202) 737-6770 (telephone)

(202) 737-6776 (facsimile)

Date: Sept 27, 2005  
JAW:ves